

# Notice of Allowability

Application No.

10/049,434

Examiner

Minh Dinh

Applicant(s)

ASANO ET AL.

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to examiner's amendment authorized on 11/28/06.
2. ☒ The allowed claim(s) is/are 1,2,5-12,15,16,21,23-35 and 37.
3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☒ All b) ☐ Some\* c) ☐ None of the:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☒ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.  
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
  - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
    - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
  - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

## Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08),  
Paper No./Mail Date 10/06/06, 4/10/07
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413),  
Paper No./Mail Date \_\_\_\_\_.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_.

### **EXAMINER'S AMENDMENT**

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Raymond Churchill on 11/28/06.

The claims have been amended as follows:

1. (currently amended) An information recording device for recording the information on a recording medium, comprising:

memory means for holding a node key unique to each node of a hierarchical tree structure having a plural number of such information recording devices, operating as leaves, and a leaf key unique to each information recording device, said memory means also holding a key renewal block formed as renewal key storage data decryptable using at least one of the node key and the leaf key; and

encryption means for decrypting the key renewal block decryptable using at least one of the node key and the leaf key provided in said information recording device to calculate an encrypting key used in encrypting data to be stored in said recording medium; said encryption means encrypting the data to be stored in said recording medium using the calculated encrypting key;

said encryption means detecting, in encrypting and storing content for said recording medium, the latest usable key renewal block from key renewal blocks stored in said recording medium and from the key renewal block stored in said memory means of the information recording device itself; said encryption means encrypting the data to be stored on said recording medium using the encrypting key obtained on decrypting the detected latest usable key renewal block,

wherein said information recording device ~~is configured for executing~~executes processing of writing the latest usable one of the key renewal blocks stored on said recording medium and the key renewal block stored in the memory means of the information recording device itself, in the memory means of the information recording device itself, in case the latest usable key renewal block is the key renewal block stored in the recording medium and the latest key renewal block is not as yet stored in the memory means of the information recording device itself,

and wherein said information recording device executes the processing of writing the latest usable one of the key renewal blocks stored on said recording medium and the key renewal block stored in the memory means of the information recording device itself on the recording medium in case the latest usable key renewal block is the key renewal block stored in the memory means of the information recording device itself and the latest key renewal block is not as yet stored on the recording medium.

3. (cancelled)

7. (currently amended) An information reproducing device for reproducing the information from a recording medium, comprising:

memory means for holding a node key unique to each node of a hierarchical tree structure having a plural number of such information reproducing devices operating as leaves, and a leaf key unique to each information reproducing device, said memory means also holding key renewal blocks each formed as renewal key storage data decryptable using at least one of the node key and the leaf key; and

encryption means for decrypting the key renewal block decryptable using at least one of the node key and the leaf key provided in said information reproducing device to calculate an encrypting key used for decrypting cipher data stored in said recording medium; said encryption means decrypting the cipher data stored in said recording medium using the calculated encryption key;

said encryption means detecting, in processing of decrypting the cipher data stored in said recording medium, a latest one of the key renewal block stored in the recording medium and the key renewal block stored in the memory means of the reproducing device itself, which has a version coincident with the version of the encrypting key of the content to be reproduced; said encryption means executing the decrypting processing of the cipher data stored on the recording medium using the encrypting key obtained by the processing of decrypting the detected key renewal block; and

renewal means for comparing, in accessing the recording medium, a version of a key renewal block stored in the recording medium to that of a key renewal block owned by the reproducing

device itself, and for writing a key renewal block of a new version in the recording medium, if the key renewal block of the new version is the key renewal block stored in the memory means of the reproducing device itself, and the key renewal block of the new version is not as yet stored on the recording medium.

12. (currently amended) An information recording method in an information recording device adapted for recording the information for a recording medium, said information recording device holding a node key unique to each node of a hierarchical tree structure having a plural number of such information recording devices, operating as leaves, and a leaf key unique to each information recording device, said method comprising:

a step of detecting a latest usable one of key renewal blocks stored in the recording medium and the key renewal block stored in said memory means of the information recording device itself;

a step of decrypting the detected latest usable key renewal block, at said detection step, using at least the node key or the leaf key held in said information recording device, to calculate the encrypting key used in encrypting data stored in said recording medium; and

a step of encrypting recording data for said recording medium, using the calculated encrypting key, to store the encrypted data on the recording medium,

wherein, in case the detected latest usable key renewal block is the key renewal block stored in the recording medium and the latest key renewal block has as yet not been stored in the memory means of the information recording device itself, said detection step executes the processing of writing the

latest key renewal block in said memory means of the information recording device itself,

and wherein, in case the detected latest usable key renewal block is the key renewal block stored in the memory means of the information recording device itself and the latest key renewal block has as yet not been stored in the recording medium, said detection step executes processing of writing the latest key renewal block in said recording medium.

13. (cancelled)

15. (currently amended) An information reproducing method in an information recording device adapted for recording the information for a recording medium, each of a plurality of such devices holding a node key unique to each node of a hierarchical tree structure having the plural respective information recording devices operating as leaves, and a leaf key unique to each information recording device, said method comprising:

a step of acquiring version information of an encrypting key for content being reproduced, stored in a recording medium;

a step of detecting a latest one of a key renewal block stored in the recording medium and a key renewal block stored in a memory means of the recording device itself, which has a version coincident with the version of the encrypting key of the content to be reproduced;

a step of generating an encrypting key using at least one of the node key and the leaf key by decryption processing of a key renewal block as detected by said detection step; and

a step of decrypting cipher data stored in the recording medium using the generated encrypting key; and

a step of comparing, in accessing the recording medium, a version of a key renewal block stored in the recording medium to that of a key renewal block owned by the reproducing device itself, and for writing a key renewal block of a new version in the recording medium, if the key renewal block of the new version is the key renewal block stored in the memory means of the reproducing device itself, and the key renewal block of the new version is not as yet stored on the recording medium.

2. References CA and CB listed in the information disclosure statement filed 4/10/07 are not considered because they are not in English and no translation has been provided.

3. The following is an examiner's statement of reasons for allowance. The present invention is directed to: (i) an information recording device which selects a latest key renewal block between a key renewal block stored on the recording device and a key renewal block stored on a recording medium, derives an encryption key using the latest key renewal block, encrypts information to be recorded using the derived encryption key, and records the encrypted information on the recording medium (claims 1, 12, 21 and 35); and (ii) an information reproducing device which select a latest key renewal block between a key renewal block stored on the information

reproducing device and a key renewal block stored on a recording medium, derives a decryption key using the latest key renewal block, and decrypts information from the recording medium using derived decryption key (claims 7, 15 and 28). More specifically, independent claims 1, 12, 21 and 35 identify the uniquely distinct features: if the key renewal block stored on the recording device is not the latest key renewal block, the key renewal block stored on the recording medium will be stored on the recording device; and if the key renewal block stored on the recording medium is not the latest key renewal block, the key renewal block stored on the recording device will be stored on the recording medium. The closest prior art, Lotspiech (6,609,116), discloses an information recording device and method which store a key renewal block of the latest version stored on the recording device on a recording medium; however, the key renewal block stored on the recording medium of Lotspiech can only be as current as the key renewal block stored on the recording device, and therefore, will not be stored on the recording device. Another prior art, Asano et al. (EP 1 008 989 A2), discloses an information recording device and method which store a key renewal block of the latest version stored on a recording medium on a recording device; however, the key renewal block stored on the recording medium of Asano is not supposed to be updated, and therefore, the key



renewal block stored on the recording medium will not be stored on the recording medium.

Independent claims 7, 15 and 28 identify the uniquely distinct features: comparing the version of a key renewal block stored on the information reproducing device to that of a key renewal block stored on a recording medium, and writing a key renewal block of a new version in the recording medium, if the key renewal block of the new version is the key renewal block stored in the memory means of the reproducing device itself, and the key renewal block of the new version is not as yet stored on the recording medium. The closest prior art, Asano et al. (EP 1 008 989 A2), discloses an information reproducing device which compares the version of the key renewal block stored on the reproducing device to that of a key renewal block stored on a recording medium; however, Asano only updates the key renewal block stored on the reproducing device.

The prior art, taken either singly or in combination, fails to anticipate or fairly suggest the limitations of applicant's independent claim, in such a manner that a rejection under 35 U.S.C 102 or 103 would be proper. The claimed invention is therefore considered to be in condition for allowance as being novel and nonobvious over prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays,

should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MD/  
Minh Dinh  
Examiner  
Art Unit 2132

06/08/06

  
GILBERTO BARRON JR.  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100